ABSTRACT OF THE DISCLOSURE

A method for authenticating a message recipient and for secure communication of messages from a sender to the message recipient through a server, the method being carried out by one or more data processing systems in accordance with instructions carried on one or more computer readable media. The message is communicated by sending message data encrypted with a symmetric key algorithm, a private key for the encryption algorithm being generated by hashing first data, to the message recipient through a server. The message recipient is authenticated by the exchange of second data encrypted with the encryption algorithm, an authentication key for said encryption algorithm being generated by hashing third data. The first and second data include a password, which has previously been provided to the message recipient over a separate secure channel. The first and third data are hashed with an encryption algorithm defined hash algorithm using said encryption algorithm and based on Merkle's meta-method for hashing.